PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Monografia de final de curso

INFLUÊNCIA DO STAKING E DAS TARIFAS DE REDES BLOCKCHAIN NA VIABILIDADE DAS CRIPTOMOEDAS NO LONGO PRAZO

Enfoque na segunda geração das criptomoedas

Cesar Krauss Silva Campello

Matrícula: 1410701

Departamento de Economia – PUC-Rio

Orientador: Rafael Guthmann

Rio de Janeiro

Dezembro de 2020

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO

DEPARTAMENTO DE ECONOMIA

MONOGRAFIA DE FINAL DE CURSO

INFLUÊNCIA DO STAKING E DAS TARIFAS DE REDES BLOCKCHAIN NA VIABILIDADE DAS CRIPTOMOEDAS NO LONGO PRAZO

Cesar Krauss Silva Campello

Matrícula: 1410701

Orientador: Rafael Guthmann

Dezembro de 2020

Declaro que o presente trabalho é de minha autoria e que não recorri para realizá-lo, a nenhuma forma de ajuda externa, exceto quando autorizado pelo professor tutor.

As opiniões expressas neste trabalho são de responsabilidade única e exclusiva do autor.

Sumário

I. Introdução 5
II. Histórico da moeda como um registro contábil 7
Paralelo entre as criptomoedas da segunda geração e o ouro e a prata 9
III. Aspectos econômicos da validação de dados 12
O enigma do duplo pagamento e a descentralização 12
Contexto histórico e tecnológico 13
Como funcionam os incentivos econômicos em redes blockchain 15
Mecanismo de consenso 15
Proof of work 16
Proof of stake 19
Concorrência entre moedas 22
IV. Aspectos teóricos 23
Abba Lerner e a Teoria Estatal da Moeda 24
Tarifas nas redes blockchain da segunda geração 27
V. Conclusão 29
VI. Referências bibliográficas 31

I. Introdução

O ano de 2014 viu surgir a segunda geração das criptomoedas com a criação da rede ethereum abrindo-se um novo espectro de possibilidades de inovação nesta área. Outras redes concorrentes vêm sendo criadas desde então, fazendo com que a criptoeconomia passasse a contar com uma diversidade maior de ativos e serviços. O que diferencia a segunda da primeira geração de criptoativos é a possibilidade de se processar aplicações diversas em suas redes blockchain e não apenas transações.

Procuramos investigar nesta monografia se as criptomoedas da segunda geração comportam-se de maneira distinta em relação às demais e se suas características lhes ofereceriam uma âncora para tornarem-se mais duradouras uma vez que tais moedas são necessárias como meio de pagamento para as tarifas pagas pelos aplicativos em sua própria rede. Levantamos aqui o questionamento sobre em que medida tal demanda por essas criptomoedas não seria uma maneira de produzir o mesmo truque criado em favor das moedas nacionais quando se obriga o cidadão a pagar impostos somente com a moeda emitida pelo governo e com isso se gera uma demanda forçada.

As criptomoedas surgiram em 2009 num contexto de grande insatisfação social com o disfuncionalidade do mercado financeiro mundial que acabava de entrar em crise com o estouro da bolha imobiliária norte-americana. Os interesses dos operadores das finanças não estariam alinhados com os de seus clientes, nem com os da sociedade em geral e ninguém se sentia incentivado ou responsabilizado a cuidar para que todo o sistema funcionasse harmoniosamente.

Os programadores e criptógrafos que primeiro trabalharam em cima do artigo divulgado pelo autodenominado Satoshi Nakamoto tinham em mente desenvolver uma tecnologia que permitisse ao cidadão comum a liberdade de escolha a respeito de qual moeda deseja utilizar para poupar e para efetuar pagamentos, que não fosse confiscável pelo governo e que não desse margem à censura de qualquer espécie. Além disso, os cidadãos ficariam invulneráveis aos abusos cometidos pelos governos com suas moedas nacionais.

Em 2014, foi lançada a ethereum que viria a criar um ecossistema de aplicações que são processadas em sua rede. Agora além de moedas não confiscáveis e não censuráveis, as redes blockchain passaram a permitir o processamento e a hospedagem de serviços que não podem sofrer intervenção do Estado, do setor privado e de hackers. Outras redes com semelhante característica foram lançadas na sequência tais como NEO, NEM, Komodo, Ontology e muitas outras. A essas damos o nome de redes blockchain da segunda geração e é nelas que estamos interessados neste trabalho.

Uma das melhores linhas de explicação desse argumento é estabelecer um paralelo com a Teoria Estatal da Moeda, sem esquecer, é claro, que estamos lidando com criaturas diferentes. Isto nos leva a uma abordagem que consideramos estimulante que é a construção de um fio condutor entre as criptomoedas desta classe e às duas outras formas principais de moeda que foram os metais e a moeda fiduciária. A partir desta linha de continuidade histórica ficará claro que cada tipo de padrão monetário é produto do seu tempo e que por isso representa as aspirações dos indivíduos que a adotarão e se encaixa na visão de mundo que se desenvolve em cada sociedade e em cada época.

O aspecto histórico não constitui de forma alguma uma divisão ou dispersão dos objetivos desta monografia. Como iremos demonstrar na seção seguinte, isto faz parte da fundamentação teórica que pretendemos estabelecer.

II. Histórico da moeda como um registro contábil

O papel-moeda surgiu inicialmente como uma representação dos metais preciosos criada por casas bancárias. Os clientes depositavam principalmente ouro, mas também prata, e recebiam em contrapartida um papel que servia como documento de comprovação do depósito, mas que também servia como meio de troca: o portador poderia fazer compras com tal papel ou efetuar saques em um banco privado em outra cidade. Tal tecnologia facilitava a circulação de riqueza já que não era fácil e seguro transportar valores ou guardá-los em casa.

É incerto e desnecessário determinar onde exatamente surgiu este fenômeno, o que importa é que a tradição que prevaleceu historicamente foi aquela que desenvolveu-se na Europa ocidental da época do Renascimento. O desenvolvimento financeiro foi consequência do crescimento do comércio, porém um alimentou o outro, já que também os comerciantes encontraram financiamento de seus empreendimentos nas incipientes instituições financeiras presentes nas grandes cidades. Com o passar do tempo, os bancos se sentiam encorajados a oferecer mais crédito a medida em que se incorporava a percepção de que era possível emitir muito mais moeda bancária do que a quantidade de metais presentes nos cofres.

Paralelamente à consolidação do setor financeiro e do papel-moeda, o surgimento dos estados nacionais também foi consequência do boom comercial e teve nos comerciantes seus principais apoiadores e interessados. Dentre as diversas motivações, importa mencionar para este estudo, a padronização dos pesos e medidas e das moedas nacionais, já que atrapalhava ao empresário da época a existência de moedas diferentes em cada feudo.

Sobre a falta de padronização neste período na esfera monetária é possível levantar alguns tópicos interessantes. De um lado havia os feudos, cunhando suas respectivas moedas metálicas, com distintos pesos, desenhos e nomenclatura. E do outro, havia cada banqueiro emitindo seus respectivos certificados de depósito, que nada mais eram do que recortes de determinadas quantidades de moeda. Some-se a isso as diferentes paridades que podiam existir entre as moedas de ouro e de prata, que não necessariamente contavam com uma cotação fixa entre uma e outra, mas ao contrário,

variavam conforme a escassez dos respectivos metais[1]. Sem falar do aparecimento das moedas de cobre e de outros metais que surgiram para facilitar o troco e as compras de valores pequenos, bem como da prática desonesta de raspar as moedas e do uso de ligas metálicas com pureza diferente em cada região.

Não é difícil imaginar que tal ausência de padrões gerasse incerteza e fricção desnecessárias na economia do dia a dia e, por isso, os estados nacionais, cada um ao seu tempo, trataram de protagonizar em mais uma etapa do desenvolvimento da moeda, trazendo para si a responsabilidade de serem os únicos emissores de papel-moeda, que nada mais era que um certificado lastreado em uma quantidade de ouro que dava ao detentor o direito de ir numa repartição do governo sacar tal quantia em metal. No entanto, diferentemente da moeda emitida pelos bancos privados, a moeda nacional agora era (ou melhor, deveria ser) totalmente lastreada em uma quantidade de ouro e não caberia ao soberano emitir papel-moeda numa quantidade superior ao que detinha em seus cofres. Pelo menos esse era o contrato social.

No entanto, as constantes emissões de papel-moeda lastreado em ouro, porém abaixo do par, com o intuito de custear o orçamento do Estado, contribuiu para que o cidadão, a contragosto, passasse a associar o seu patrimônio em espécie não mais com o que ele possuía em metal, mas a essa referência abstrata do número escrito no papel. O papel-moeda aos poucos transformava-se em moeda papel.

Os bancos privados continuaram, como se sabe, a oferecerem seus serviços, porém agora a moeda bancária emitida nada mais era do que a própria moeda nacional. Isso era possível porque cada vez mais as transações não ocorriam de mão em mão, mas dentro dos próprios registros dos bancos, de uma conta corrente de um cliente para a conta de outro. Assim, os bancos continuavam a expandir seus balanços via crédito em favor do público, como faziam antes, mas agora o que eles detinham em seus cofres era o papel-moeda. E por outro lado, o que o cidadão comum possuía era cada vez mais não

[1] Nos dias atuais, é difícil nos imaginarmos lidando com tal situação, já que estamos extremamente habituados com o fato lógico e conveniente de que dez moedas de um real equivalem a uma nota de dez reais. Contudo, como a escassez de prata e de ouro não variam necessariamente na mesma proporção, mas são determinadas por uma atividade totalmente exógena que é a mineração, então como saber ao certo, no dia a dia, quantas moedas de prata podiam ser trocadas por uma de ouro?

um objeto em si, papel ou metal, mas um registro anotado a mão num livro dentro do banco.

O progresso tecnológico dos séculos XX e XXI veio a fortalecer esse formato (surgido nos bancos medievais) da moeda como um registro. O advento da moeda eletrônica (bancária), das criptomoedas (a blockchain nada mais é do que um livro-razão eletrônico descentralizado) e agora do recente experimento da moeda digital chinesa (que não é bancária, mas um registro nos servidores do Banco Central da China, expressado nos aparelhos celulares de cada cidadão), revelou uma tendência dos formatos de moeda em se tornarem mais abstratos ainda e de não terem uma contrapartida real no mundo físico. Apesar disso, é pouco disseminada, ainda hoje, a noção de reservas fracionárias e o cidadão comum não faz a manobra mental de calcular que os bancos não teriam saldo para cobrir uma quantidade excessiva de saques de seus correntistas.

Paralelo entre as criptomoedas da segunda geração e o ouro e a prata

Qual seria o propósito de um preâmbulo histórico a respeito das duas formas principais de moeda numa monografia a respeito de criptomoedas? Procuramos traçar paralelos históricos com os padrões monetários do passado para identificar se as inovações do presente contariam com características que as permitiriam ter continuidade no longo prazo. Neste trabalho, embora em alguns momentos tratemos das criptomoedas em geral, daremos especial atenção àquelas consideradas da *segunda geração*, nomenclatura um pouco imprecisa para designar aquelas cujas redes estão mais adaptadas a processar aplicações e que surgiram com o lançamento da rede Ethereum.

Entendemos que dentro do ethos da criptoeconomia e dos criptoativistas a liberdade econômica é um valor que permeia as discussões e desperta o entusiasmo com esta nova classe de ativos que permitem que o agente econômico escolha como moeda o ativo que lhe aprouver. Assim, tornamo-nos livres da imposição da moeda estatal. Porém podemos avaliar criticamente esta possibilidade, pois quando temos liberdade de escolha, também somos livres para não escolher. Com isso, ao se dar a chance aos indivíduos de rejeitarem as moedas nacionais, também se suscita o questionamento a respeito da possibilidade de um dia algumas criptomoedas virem a ser rejeitadas. O que

garantiria aos poupadores de uma determinada criptomoeda, a certeza de que, sob qualquer circunstância, jamais aconteceria de um dia acordarem de manhã e verem sua carteira de criptoativos valer zero por causa de um boato em outro continente do outro lado do mundo?

O ouro possui demanda industrial. Quando foi padrão universal seus usuários não precisavam ter a preocupação de sua cotação depreciar até zero porque sempre haveria nobres e instituições eclesiásticas que comprariam o metal para produzir seus ornamentos. Na hipotética situação de o ouro desvalorizar-se bruscamente por razões especulativas, os artesãos que utilizavam este metal como insumo se apressariam em comprá-lo em maior quantidade, o que corrigiria o preço para cima.

Com relação ao papel-moeda, a "ancoragem" é um pouco mais sofisticada, mas também se baseia na demanda pela moeda. Em todos os países, os impostos somente podem ser pagos na moeda nacional. Se lembrarmos que de 20% a 50% das economias nacionais giram em torno dos gastos e receitas governamentais, estamos lidando com uma circulação forçada que não deixa qualquer dúvida sobre se haverá ou não demanda pela moeda nacional no dia de amanhã.

As criptomoedas da *primeira geração* são registros presentes numa rede de computadores descentralizada e contam com o efeito de rede para que se perpetuem: quanto maior o número de indivíduos se conectando, mais novos usuários se sentirão encorajados a utilizá-la. Porém, objetivamente, elas não têm uso nenhum e são vulneráveis a efeitos de manada mobilizados, por exemplo, por um boato. Diferentemente do ouro e da moeda fiduciária, esta primeira geração não conta com demanda forçada ou demanda industrial.

É nesse ponto que as criptomoedas da segunda geração se diferenciam, já que contam com uma espécie de demanda industrial. A possibilidade de se desenvolver aplicações nas redes blockchain não expande apenas a fronteira da tecnologia, mas também cria uma âncora para que esses criptoativos se tornem mais perenes. Isto porque o pagamento pela hospedagem e pelo processamento de dados dentro da rede deve ser feito com a moeda da própria rede. Assim, a tarifa de hospedagem na rede blockchain possui um efeito semelhante ao dos impostos para o papel-moeda. Neste ecossistema,

vemos que existe um tipo de demanda por esses criptoativos que vai além da demanda por meios de pagamento e de reserva de valor.

A forma de pagamento das tarifas pode variar de rede para rede, mas verificamos que a operação denominada como *staking* é uma das formas de viabilizar tanto a mineração da rede como o funcionamento dos aplicativos. A rede da criptomoeda Neo, por exemplo, conta com aplicativos de carteira que guardam Neos para que sejam gerados dividendos em uma outra moeda, denominada Gas; e esta por sua vez serve como meio de pagamento das tarifas pelo uso da rede. Assim, tais remunerações incentivam a poupança e, portanto, viabilizam a preservação do valor e redução das oscilações do preço desse ativo. Vamos discutir aqui se tais mecanismos podem ser considerados como âncoras que garantam a perenidade de uma moeda.

Para que alguém decida poupar numa criptomoeda é preciso que se tenha no horizonte a expectativa de que esta não desaparecerá do mercado. E isto é algo bastante preocupante dado que se verifica que muitos projetos não têm continuidade seja pela não formação de um público seja pela falta de lógica econômica ou mal funcionamento. Contudo, podemos relativizar tal preocupação levando-se em conta que também no mercado financeiro são emitidos diversos ativos cujos valores vão a zero em pouco tempo, como as penny stocks, debêntures de empresas insolventes e títulos de governos em dificuldades.

III. Aspectos econômicos da validação de dados

O enigma do duplo pagamento e a descentralização

Como criar um dinheiro da internet se todos os elementos do mundo digital podem ser reproduzidos infinitas vezes? Um arquivo anexado num e-mail pode ser reencaminhado para milhões de pessoas e um vídeo online pode ter milhares de visualizações. Como garantir que o possuidor de uma moeda digital da internet não irá utilizar essa mesma moeda para pagar duas vezes? O enigma do duplo pagamento era uma questão fundamental para os pesquisadores que tentavam criar uma moeda para o mundo virtual desde a década de 1990 e por isso tal moeda não poderia ser um arquivo de computador ou um código por exemplo[2].

No sistema bancário, essa questão é tratada através da centralização. Um pagamento eletrônico gera um crédito para o recebedor da moeda e um débito igual para o pagador e, com isso, a quantidade total de dinheiro entre as duas partes não aumenta a cada pagamento, pois tudo isso é processado nos servidores dos bancos envolvidos sem o controle do correntista. Ele não pode usar mais dinheiro do que possui em sua conta bancária, porque quem controla o sistema é o banco. O que os pesquisadores do assunto tentavam criar não era uma nova moeda bancária, mas uma espécie de *e-cash*, um dinheiro que pudesse ser transferido de A para B de maneira análoga ao que acontece com o papel-moeda e com as moedas de ouro, mas que fosse digital e sem um agente centralizador com potencial coercitivo.

O saldo de uma conta bancária é tão somente um registro contábil, e não há necessidade de existir uma contraparte em papel-moeda desses valores. Ao se efetuar uma transação bancária, os funcionários do banco não pegam o dinheiro que está numa gaveta com o nome do cliente e colocam-no na do beneficiário da transação. Assim, como a moeda bancária é um registro, os valores que constam nas contas correntes podem ser apagados, adulterados, ou o correntista pode ter o pleno acesso ao seus direitos de movimentação bloqueados pelo ente centralizador, que é o banco, ou pela autoridade monetária, pelos órgãos de fiscalização etc. E, sem sombra de dúvidas, esta

[2] Nakamoto, S.

é uma ferramenta bastante conveniente para governos autoritários. Então o cliente não pode alterar o registro contábil a seu bel prazer, mas o banco tem esse poder, bem como as autoridades do país.

Desta maneira, a solução para o problema viria a ser também a de criar um sistema que fosse ele próprio responsável por fazer registros contábeis, porém cujas movimentações de valores fossem computadas de maneira descentralizada, isto é, a tecnologia de registro deveria ser outra, já que os bancos utilizam servidores centrais para processar as operações de seus clientes.

Tecnologias descentralizadoras já vinham sendo desenvolvidas, em especial, as denominadas peer-to-peer (P2P), isto é, aquelas nas quais diversas máquinas processam as mesmas informações e estabelecem processos de comunicação sem que haja uma delas a governar as demais. Com isso, o mal funcionamento de uma delas não inviabiliza o funcionamento da rede como um todo. Uma rede assim, tendo dimensão internacional, não pode ser destruída por uma guerra, pela censura de um governo ou por hackers. Os pesquisadores dessas tecnologias precisavam aperfeiçoá-las de maneira a que ninguém tivesse meios para fraudar o sistema, todos tivessem incentivos microeconômicos à cooperação e os que tentassem prejudicar a rede sofressem penalizações (econômicas) por isso.

Contexto histórico e tecnológico

O clima político da época do surgimento do bitcoin era de grande descrença, principalmente nos Estados Unidos, com relação à má gestão da moeda que gerou a crise financeira em 2008 (o white paper, de Satoshi Nakamoto foi lançado em outubro de 2009) e uma crescente preocupação com privacidade e com a autodeterminação do cidadão em seus assuntos particulares. Já havia uma percepção de que os avanços tecnológicos vinham cada vez mais sendo utilizados por governos e empresas para invadir a vida privada dos cidadãos. Além disso, precisamos lembrar do contexto tecnológico daquele momento.

Já havia uma ampla disseminação da internet, não só nos computadores, mas também com o advento dos smartphones. Sistemas de pagamentos na internet como o paypal já estavam disseminados, porém todos eram processados em servidores centralizados, é claro. O software livre já possuía um peso igual ou maior do que aqueles de natureza privada e podem ser citados em particular aqueles utilizados para o compartilhamento gratuito, pirateado, de arquivos de músicas. A compreensão destes últimos facilita o entendimento inicial de como funciona uma rede blockchain e de qual era a mentalidade por trás daqueles que se aventuravam em desenvolver este tipo de programa.

Avançando mais no contexto tecnológico, softwares descentralizados de compartilhamento de arquivos musicais estão entre aquelas tecnologias que serviram de base para se criar a lógica do funcionamento dos criptoativos. Como o processamento das informações e o armazenamento das músicas é feito num número grande e desconhecido de computadores o funcionamento de uma tal rede de cooperação não pode ser censurado por uma autoridade ou por grupos de interesse. E por isso, é bastante claro que promoveram danos ao funcionamento de diversos mercados que dependiam da garantia de propriedade intelectual. Ocorreram tentativas mal sucedidas de polícias de vários países no sentido de acabar com o uso destes softwares, porém seu amplo uso e sua natureza descentralizada e global tornaram impossível a fiscalização.

Porém esses softwares, tinham um problema de natureza econômica: não havia uma maneira de gerar incentivos econômicos para os agentes empenharem seus esforços de pesquisa e de tempo a fim de promoverem a criação de novos produtos e para melhorarem os mesmos. Os desenvolvimentos ocorriam a partir de trabalho voluntário. A seguir vamos apresentar como as inovações que acompanharam o surgimento do bitcoin não foram apenas na área da tecnologia, mas também na forma como foram pensados os incentivos microeconômicos de forma a atrair para este tipo de atividade um significativo volume de capital intelectual e financeiro.

Como funcionam os incentivos econômicos em redes blockchain

Com o advento das redes blockchain, a falta de recursos financeiros foi solucionada, pois, a partir de então, os desenvolvedores de novos serviços descentralizados podem se financiar através da emissão de criptoativos. No caso do bitcoin, isso ainda não fica claro, pois sua rede não é eficiente para hospedar e processar praticamente nada além do registro das suas próprias transações monetárias. Contudo, com o avanço rápido da tecnologia, surge a rede Ethereum, com a moeda de nome ether, com a qual novas funcionalidades tornam-se viáveis. Em sua criação, foi realizado um ICO, *initial coin offering*, que nada mais é do que o lançamento das moedas da rede para compra pelo público em geral, de maneira semelhante a um IPO, promovido pelas bolsas de valores do mundo todo, só que com menor ou nenhuma regulamentação.

As moedas iniciais emitidas passam então servir como uma forma de financiamento dos desenvolvedores que irão aprimorar o funcionamento da rede. Esta não é mais uma rede para se processar apenas as transações de sua própria moeda. A partir de então, tornou-se possível lançar serviços dentro da rede ethereum e estes poderiam também se financiar, lançando seus próprios criptoativos. Com isso, as tecnologias P2P que antes avançavam com o trabalho voluntário de programadores, agora passam a estar envolvidas em um novo setor da economia. Na sequência da ethereum, outras redes com esta característica foram lançadas, dentre elas a Neo, a Cardano e a Nem. As criptomoedas que viabilizam este tipo de rede passaram ser classificadas como as da *segunda geração* deste setor. Mencionaremos a maior parte das relações econômicas envolvidas dentro de uma rede blockchain, porém focaremos naqueles aspectos mais intimamente relacionadas ao funcionamento das suas moedas.

Mecanismo de consenso

Se numa rede descentralizada não há um agente central a tomar decisões, qual é o mecanismo que os participantes utilizam para definir o que valerá para toda a rede? É preciso que haja uma maneira de se estabelecer um acordo para que todos validem as

mesmas transações, isto é, para que todas máquinas concordem com o mesmo bloco de transações a cada ciclo de processamento.

Para lidar com esta questão o criador do bitcoin, Satoshi Nakamoto, criou um mecanismo (ou algoritmo) de consenso chamado de proof of work. Posteriormente, a fim de enfrentar alguns problemas identificados neste, foi criado o proof of stake. Estes dois mecanismos são os mais utilizados nas redes blockchain, ambos possuem suas vantagens e desvantagens que serão discutidas a seguir.

Proof of work

É importante observar que foi preciso gerar incentivos para atrair agentes econômicos dispostos a oferecer poder computacional para o processamento das informações da rede. As empresas e indivíduos que ingressam nesta atividade são denominados mineradores. Eles conectam suas máquinas a uma rede, por exemplo a do bitcoin, e estas participam de uma competição, um jogo, em que o vencedor é remunerado em criptomoedas. Vamos explicar a seguir como funciona a mineração para em seguida discutir as questões econômicas envolvidas nela.

As transações são organizadas em blocos e este é o motivo do nome blockchain – cadeia de blocos. No caso do bitcoin por exemplo a cada dez minutos é processado um bloco de transações, uma lista de transações. Estas são públicas e podem ser auditadas por qualquer pessoa ou por qualquer máquina e, portanto, todo o histórico de transações de bitcoins desde o seu surgimento pode ser verificado. As transações são públicas, porém anônimas, isto é, são conhecidas as quantias movimentadas, embora não sejam nomeados os agentes envolvidos.

Cada minerador propõe à rede o seu bloco como um candidato a ser o bloco registrado. Para vencer essa competição, o minerador deverá empenhar grande poder computacional com dispêndio elevado de eletricidade para resolver um problema matemático mais velozmente do que os demais competidores. Tal procedimento visa a gerar um custo que o desincentive a propor um bloco com transações fraudulentas que invariavelmente seriam rejeitadas pelas demais máquinas. Assim, torna-se caro e difícil

tentar fraudar a rede e lucrativo colaborar com ela, já que o vencedor deste jogo é remunerado com novas emissões de bitcoin feitas pela própria rede a cada bloco processado. Um potencial fraudador despende eletricidade e depreciação dos seus equipamentos e no final das contas seu bloco é recusado pelas demais máquinas. Esse empenho gerado pelo minerador em poder computacional e energia recebe o nome de *proof of work*. Se trata de uma tecnologia anterior as criptomoedas que foi aproveitada pelos desenvolvedores do bitcoin[3].

Repare que aqui temos algumas ineficiências. Em primeiro lugar, os mineradores despendem seus esforços muito mais no sentido da competição neste jogo do que propriamente para processar as transações monetárias. A prova de trabalho não tem aplicação prática nenhuma e nem se propõe a ter. Em segundo lugar, ela está relacionada a um gasto elevado de energia elétrica e, por isso, cabem aqui todas as críticas relacionadas a questões ambientais e de aproveitamento dos recursos energéticos de um país. Em terceiro lugar, por ser uma típica atividade industrial com ganhos de escala, observa-se a concentração dessas plantas industriais nas mãos de poucos agentes. Também se verifica a concentração de empresas de mineração em locais do planeta onde os custos com eletricidade são muito baixos.

Ressaltemos aqui um outro ponto importante da forma como foi estruturada essa atividade que tem repercussões no comportamento da moeda. O minerador tem seus custos em energia elétrica e em tecnologia. Parte das criptomoedas que ele receber terão que ser trocadas por moeda fiduciária para arcar com estas despesas. Portanto, repare o leitor que no funcionamento descrito aqui não há nenhum mecanismo intrínseco que incentive ou obrigue os agentes a pouparem bitcoins ou a usarem-nos como meio de pagamento. Traduzindo isto para uma pergunta: qual seria a demanda mais intrínseca (endógena) do bitcoin?

No caso do ouro, por exemplo, pode-se utilizá-lo como moeda, mas ele também conta com uma demanda industrial (no passado joias e artefatos em templos, e hoje também na eletrônica). Se, por razões meramente especulativas, o preço do ouro despenca, os industriais que o dependem dele como insumo se apressarão em adquiri-lo em maior

[3] Nakamoto, S.

quantidade, favorecendo a uma correção desta queda. O uso industrial antecede o monetário. Já no caso da moeda fiduciária, estatal, as leis relacionadas ao curso forçado geram demanda pela moeda para que os agentes econômicos só sejam capazes de transacionar com a moeda nacional. Um proprietário de imóvel no Brasil só consegue pagar em reais o seu IPTU. Mesmo que a prefeitura esteja endividada, ela recusará pagamentos em dólar, ouro ou criptomoedas. Temos aqui então uma demanda forçada por reais.

Inexiste tal mecanismo no caso das criptomoedas que utilizam o proof of work. O que existe no caso do bitcoin é uma grande quantidade de corretoras de criptomoedas em que ele é par nas transações. Nelas a maior parte das criptomoedas pode ser adquirida através de pagamentos em bitcoin. Não se trata exatamente de uma demanda forçada, portanto, mas de algo que é alimentado pelo próprio frenesi em torno do mercado de criptomoedas e que sem sombra de dúvidas sustenta as expectativas em torno desta moeda enquanto essas corretoras mantiverem essa política.

Uma outra questão que podemos suscitar é sobre a quantidade de mineradores, ou dito de outra forma, o que determina a quantidade de poder computacional que é empregada numa rede blockchain? A resposta está no preço da moeda e, portanto, nas possibilidades de lucro do empresário da mineração. Quanto maior a valorização em dólares de uma criptomoeda, maior será a quantidade de poder computacional que o mercado irá alocar para minerá-la. Cada rede blockchain remunera os mineradores segundo uma regra diferente. No caso do bitcoin, por exemplo, a rede gera novas moedas em quantidades fixas por bloco minerado.

Porém o que ocorreria no caso de uma queda do valor de uma criptomoeda? Será que a atividade de mineração tornar-se-ia inviável? Na verdade, desenvolveu-se equipamentos capazes de minerar mais de um tipo de criptomoeda e os novos criptoativos que são lançados já procuram estar adaptados a algum tipo de máquina disponível no mercado. No dia a dia deste mercado é perfeitamente normal minerar moedas diferentes conforme oscilam os preços relativos e conforme variam as quantidades de competidores em cada mercado.

Foi mencionado acima a possibilidade de concentração na atividade mineradora, o que abre portas para ações orquestradas por alguns mineradores que concentram grande poder computacional. Recentemente, no segundo semestre de 2020, ocorreu uma situação difícil de afirmar se foi intencional ou não. O governo chinês iniciou um processo de fiscalização na principal corretora do país a Okex, proibindo o saque durante o período da auditoria[4]. Isso fez com que os mineradores chineses não pudessem vender suas moedas para pagar suas contas de eletricidade. Continuaram minerando, supostamente ficando em dívida com as companhias de eletricidade e não participaram da força vendedora nos mercados de compra e venda de criptoativos durante este período. Esta é uma das linhas de explicação do motivo pelo qual o bitcoin valorizou-se mais de 80% desde o início da fiscalização. Não importa aqui identificar se tal acontecimento foi orquestrado ou não, mas apontar que existe esta vulnerabilidade econômica em algumas criptomoedas que validam transações através do algoritmo do proof of work.

Proof of stake

Proof of stake é um mecanismo de consenso entre os validadores de blocos de transações de uma blockchain. A tradução mais utilizada para o português é *prova de participação*, apesar de também podermos traduzir o verbo *to stake* como *apostar*. Embora a tradução seja imprecisa, como verifica-se também na criptoeconomia o uso do termo *stakeholders* para se referir àqueles se candidatam a validadores, a compreensão do termo proof of stake fica mais fácil. Assim, *staking* consiste em congelar uma quantidade de criptomoedas que servirá de colateral para a operação de validação de dados. Um dos participantes será selecionado como o validador de um novo bloco de transações. Tal escolha será definida por um critério probabilístico que varia bastante de rede para rede, mas que geralmente envolve a quantidade de criptomoedas aportada e o tempo em que elas foram colocadas em staking. Quanto mais moedas e mais tempo, maior a probabilidade de ser selecionado para validar um novo bloco e com isso receber um pagamento na criptomoeda nativa da própria rede.

[4] Asia Times

Se o participante do processo de staking se comportar mal e tentar aprovar uma transação fraudulenta, ele perde as criptomoedas colocadas como colateral. Por outro lado, se colaborar com a rede e validar um bloco corretamente, recebe como payoff um pagamento em moedas da própria rede que são geradas a cada novo bloco validado. Cria-se assim uma espécie de screening no qual os participantes que aportarem maior quantidade por maior tempo são remunerados com probabilidades maiores de serem os responsáveis pela validação e com isso de receberem o prêmio.

Aqui podemos reparar que há um desdobramento claro no plano econômico. No proof of stake os candidatos a validadores de blocos são incentivados a poupar criptomoedas para participar da atividade de staking, enquanto no proof of work o incentivo para os mineradores é o de gastar imediatamente as moedas recebidas no processo de mineração para cobrir os custos de eletricidade. Sendo assim um dos mecanismos incentiva a acumular cada vez mais moedas e o outro a desfazer-se delas. O algoritmo do proof of work gera intrinsecamente uma força vendedora no mercado, sendo, portanto, uma força que pressiona os preços para baixo. Já o proof of stake se mostra como uma força acumuladora e que gera uma pressão dos preços para cima.

Milhares de criptomoedas já foram criadas neste curto período de dez anos da criptoeconomia e boa parte delas já viu seu valor ir a zero e a rede toda desaparecer. Então não estamos falando de uma preocupação secundária para este setor. O staking funciona como uma âncora para a perpetuação da moeda, isto é, ele contribui para a escassez de moedas em circulação e o proof of work contribui para a abundância de moedas. Contudo, é claro que estas não são as únicas forças que atuam para cima ou para baixo nos preços dos criptoativos. Desta maneira, quanto mais o preço da moeda se eleva mais agentes econômicos se interessam por se candidatar a validar novos blocos de transações e a rede se torna mais robusta.

Há mais variações de implementações do algoritmo do proof of stake do que do proof of work (e há também redes que usam os dois algoritmos). Porém, de maneira geral, todos que participam do processo de staking contribuem com poder computacional para o processamento da rede. Em algumas redes existem as stake pools como é o caso da Cardano. Nesta forma de staking, o participante entra num pool de staking (uma espécie de coletividade) no qual um grupo de stakeholders processam juntos as

transações e concorrem em conjunto para validar novos blocos, aumentando suas chances.

Em termos de gasto de poder computacional, o proof of stake é bem menos dispendioso que o proof of work e de maneira geral não requer a construção de uma *fazenda* de mineração (um termo curioso que é usado para uma instalação de máquinas que participam da mineração proof of work), sem contar o baixo consumo de eletricidade.

Um outro tópico interessante, que às vezes está relacionado ao algoritmo do proof of stake, é o poder de voto dentro de redes blockchain. Quanto mais criptomoedas nativas da rede um stakeholder dispuser, maior poder de voto ele terá para determinar mudanças dentro de redes que ainda estão em processo de amadurecimento (quase todas) ou mesmo de votar em favor de um validador de transações ou de um pool. Neste tópico, cada rede apresenta suas peculiaridades e é impossível identificar um padrão. O que importa ressaltar é que dentro do proof of stake há ainda este outro incentivo a poupar. Como um exemplo, podemos mencionar que uma das criptomoedas da rede Neo é dedicada a participação neste mecanismo de voto e a outra voltada ao pagamento de tarifas e remuneração dos validadores.

O proof of stake é tido como um algoritmo mais veloz do que o proof of work, sendo capaz de processar um volume maior de transações por bloco, chegando a ser mais eficiente em alguns casos do que os processos utilizados pelas operadoras de cartão de crédito para registrar transações. Esta questão, contudo, vem sendo bem encaminhado pelo bitcoin que criou uma espécie de segundo camada de operações chamada de *lightening network*. Nela as operações ocorrem fora da cadeia de blocos, em redes paralelas que periodicamente se conectam à blockchain do bitcoin e zeram débitos e créditos efetuados. Esta segunda camada funciona basicamente como se fosse uma pequena rede de livros-razão que processam um conjunto menor de transações cada uma, a fim de não sobrecarregar a rede principal.

Concorrência entre moedas

Encerramos este capítulo, ressaltando a curiosa observação de que na criptoeconomia se manifesta de maneira mais clara o que Hayek denominou de concorrência entre moedas[5]. As criptomoedas e suas redes competem pela melhor tecnologia para processar transações, para implementar serviços, para garantir privacidade ou para se adaptar a determinados nichos de mercado. A disputa entre os algoritmos proof of work e proof of stake é apenas um aspecto dessa competição.

Podemos citar diversos exemplos desse processo de concorrência tecnológica. Enquanto a criptomoeda waves promete ser capaz processar um volume descomunal de transações, monero e zcash se encaixam no nicho de mercado da dark web, sendo impossíveis de serem rastreadas. O bitcoin se coloca como a mais segura das criptomoedas por ser a mais testada e a que possui a maior rede. Neo oferece a oportunidade aos desenvolvedores de implementar seus serviços utilizando quase todas as linguagens de programação. E Arcade City se apresenta como uma curiosa rede na qual funciona a concorrência descentralizada do serviço de transporte Uber.

Da mesma maneira, os fundamentos microeconômicos dos dois principais algoritmos de consenso que estudamos neste capítulo influenciam nesta concorrência, determinando uma guerra de posições nas disputas por fatias de mercado da criptoeconomia e de seus nichos. No capítulo seguinte estudaremos os aspectos econômicos relacionados às tarifas de transação, numa abordagem mais teórica e num certo sentido mais interessante, já que estabelece um paralelo entre as criptomoedas e as moedas fiduciárias. Tais comparações são importantes para compreender que os criptoativos não surgiram com fundamentos econômicos tão novos quanto parecem e que os economistas podem encontrar bases teóricas que já existem na literatura econômica.

[5] Hayek, F. Denationalisation of Money.

IV. Aspectos teóricos

A fim de estabelecer um paralelo com a moeda estatal, será de grande utilidade a Teoria Estatal da Moeda, originalmente proposta por Georg Knapp, mas que nos interessa mais na interpretação de Abba Lerner, devido à sua objetividade dentro do tópico a ser demonstrado. Em ambos os autores, o dinheiro é entendido como uma "criatura da lei". O objetivo aqui não é o de derivar este trabalho num aprofundamento excessivo nesta teoria, nem tão pouco estabelecer um posicionamento contrário ou a favor. O que se busca é apresentar o fenômeno da demanda forçada via impostos, que é um truque (nas palavras de Abba Lerner) que ancora a moeda fiduciária no sentido da preservação de seu valor e continuidade de seu uso.

As redes blockchain da segunda geração incentivam os agentes envolvidos a pouparem na sua moeda, recebendo em troca uma espécie de dividendo. A rede Neo, para citar um exemplo, conta com um processo de validação de transações que remunera por meio de uma outra criptomoeda, denominada Gas, os usuários que guardarem uma determinada quantia em Neos em carteiras eletrônicas específicas. Mediante tal poupança o usuário se insere dentro do mecanismo eletivo dos agentes que validarão as transações da rede. A medida em que a rede cresce (bem como o valor da sua criptomoeda) mais agentes são incentivados a ingressarem neste mecanismo eletivo e de obtenção de dividendos.

Estamos tratando, portanto, de uma espécie de monopólio, com o qual o criptoativo conta, dentro da sua própria rede, para a tarefa de mantê-la funcionando. Uma outra situação em que ocorre esta exclusividade é no caso da cobrança de tarifas pela manutenção dos serviços que são processadas dentro de uma rede. Na Neo há jogos funcionando, corretoras descentralizadas, sites de swap de moedas, um serviço de registro de domínios com a terminação *.neo* e vários outros serviços. Cada um deles precisa pagar uma tarifa em Gas para registrar-se, e outra para continuar funcionando. E com o advento do De-Fi (*descentralized finance*)[6] esta âncora tende a se tornar ainda mais forte.

[6] Foram criados pools de liquidez para sites de swap e para corretoras descentralizadas. Estas já existiam há alguns anos, porém não vingavam porque não tinham liquidez. Com o De-Fi é possível bloquear

É certo, no entanto, que as criptomoedas contam com o chamado "efeito de rede", isto é, quanto maior o número de usuários, maior a solidez da moeda. Dito de outra maneira, se um conjunto grande de pessoas a utiliza em transações comerciais, financeiras e contratuais, mais improvável se torna a perspectiva de que haja uma fuga deste ativo em curto espaço de tempo. A bitcoin evidentemente tem essa como sua principal força já que ela foi a primeira moeda e é a mais conhecida. Além disso, consta como par nas transações das principais corretoras de criptomoedas. Contudo, nosso foco não será neste efeito. Nossa atenção estará voltada para o peso que aquela demanda forçada, mencionada anteriormente, possui na viabilidade da moeda a longo prazo.

Pode parecer estranho aplicar a noção de demanda forçada dentro do universo das criptomoedas, já que os desenvolvedores de serviços descentralizados podem instalá-los em qualquer rede que ofereça melhores preços de tarifas e assim tenderíamos a uma dispersão infinita dos serviços em infinitas redes. Porém, o que acontece é que as redes com maior poder computacional tendem a ser mais seguras e eficientes e os aplicativos acabam por se concentrar nas maiores.

Abba Lerner e a Teoria Estatal da Moeda

Em The Origin of Money, Karl Menger propõe que a origem do dinheiro é de natureza social e que o reconhecimento do Estado seria uma etapa posterior à aceitação pela sociedade:

> *"Money has not been generated by law. In its origin it is a social, and not a state-institution. Sanction by the authority of the state is a notion alien to it. On the other hand, howeyer, by state recognition and state regulation, this social institution of money has been perfected and adjusted to the manifold and varying needs of an evolving commerce, just as custumary rights have been perfected and adjusted by statute law"*[7].

criptomoedas numa plataforma e obter *juros* por isso. Por outro lado, é possível tomar emprestado nestas plataformas para operar alavancado em corretoras descentralizadas.

[7] Menger, K. On The Origin of Money.

Embora tenham sido infrutíferas as buscas por se estabelecer as origens do dinheiro a visão de Menger parece ter coerência histórica, já que algumas sociedades primitivas já contavam com formas rudimentares de moeda. A determinação pelo Estado de um formato de moeda para toda uma nação viabiliza o funcionamento de um conjunto mais sofisticado de relações comerciais, conferindo liquidez para aquele ativo escolhido. Seja qual for a origem do dinheiro, se faz necessária a formalização de um tratamento teórico para as moedas nacionais

A Teoria Estatal da Moeda foi proposta originalmente por Georg Friedrich Knapp em 1905, porém interessam em especial algumas observações do economista Abba Lerner devido a sua simplicidade e coerência de raciocínio. Segundo proposição inovadora de Knapp, a moeda seria uma *criatura da lei* e passaria a existir a partir do momento em que o Estado reconhece determinada forma de moeda e a impõe ao comércio e ao cumprimento de contratos, o que é entendido pelo termo *curso forçado*.

Assim, abre-se caminho para o papel-moeda deixar de ser uma mera representação de um peso em metal para passar a ser ele mesmo o dinheiro. Nas palavras de Abba Lerner:

> *"Money (...) is what we use to pay for things. The basic condition for its effectiveness is that it should be generally acceptable. Its transformability into gold and the guarantee of this possibility of gold backing (...) are nothing but historical accounts of how acceptability came to be established in certain cases. These were possibly the only ways in which general acceptability could be established prior to the development of the well-organized sovereign national states of modern times. General acceptability had to be transferred in some such way from something which had already acquired it in the course of history. But if general acceptability could be established in any other way these historical methods would no longer be necessary or relevant".*[8]

No início do século XX, o que se verificava era que a ideia do papel-moeda representando um peso em metal já não traduzia de fato como funcionava o padrão monetário vigente. Havia diversas maneiras de lidar com o padrão-ouro dependendo do país. Em muitos países o Estado supostamente garantia que as notas representavam um determinado peso em ouro, mas já não efetuava a conversão pelo metal. Noutros, eram feitas emissões muito além do que se tinha estocado em ouro. Desta forma, o padrão-

[8] Lerner, A. Money as a Creature of the State.

ouro acabava por ser uma ilusão que tacitamente todos aceitavam viver para se sentirem mais seguros com a moeda que possuíam.

No entanto, à medida que o padrão-ouro se dissolvia e os governos deixavam de adotá-lo, a moeda passa a ser o papel-moeda sem lastro. Porém não bastava o Estado meramente declarar a obrigatoriedade de aceitação das suas notas de dinheiro para pagamentos e liquidação de contratos, pois o valor da moeda que antes era a resultante da oferta e da demanda por ouro, agora passa a ser determinado pelo valor em relação a moedas de outros países. Antes as moedas nacionais (libras esterlinas, mil-réis, etc.) eram tão somente recortes de uma mesma moeda que era o ouro que acabava sendo a moeda internacional.

O que Abba Lerner deixa claro é que não basta definir um ativo qualquer para que ele seja o dinheiro do país. O curso forçado deve envolver o fato de que os pagamentos de tributos só poderão ser feitos na moeda nacional, já que em momentos de crise e de descrédito da moeda, os agentes econômicos realizarão suas transações comerciais e contratuais em outras moedas, mesmo que declarem em notas fiscais e contratos que a transação está sendo feita na moeda oficial. É claro que o curso forçado em transações do setor privado é fundamental para a forçar a circulação da moeda, mas importa ressaltar para esta monografia e para o paralelo que se deseja estabelecer que os impostos são a âncora principal para que o papel-moeda funcione como moeda nacional. Vejamos como Abba Lerner aborda este tópico:

> *"The modern state can make anything it chooses generally acceptable as money and thus establish its value quite apart from any connection, even of the most formal kind, with gold or with backing of any kind. It is true that a simple declaration that such and such is money will not do, even if backed by the most convincing constitutional evidence of the state's absolute sovereignty. But if the state is willing to accept the proposed money in payment of taxes and other obligations to itself the trick is done. Everyone who has obligations to the state will be willing to accept the pieces of paper with which he can settle the obligations, and all other people will be willing to accept these pieces of paper because they know that the taxpayers, etc., will accept them in turn (...). What this means is that whatever may have been the history of gold, at the present time, in a normally well-working*

> *economy, money is a creature of the state. Its general acceptability, which is its all-important attribute, stands or falls by its acceptability by the state".*[9]

A citação acima também é apresentada por Gustavo Franco, de quem extraímos o termo *âncora* quando ele toca neste mesmo assunto:

> *"*Sim, a confiança é parte relevante da ideia de moeda, e de muitas maneiras profundas, mas a obrigatoriedade de aceitar, decorrente de lei, o curso legal - na medida aplicável também ao Estado, no recebimento dos impostos - parece oferecer uma boa "âncora" para a aceitação, ainda que não haja qualquer garantia sobre o poder de compra da moeda, ou sobre *quanta* moeda de pagamento há de ser empregada para se obter mercadorias e serviços. Os fundamentos econômicos do Estado emissor também contam e, na verdade, não é outra a base da "confiança", que está longe de ser cega e surda. Para a moeda de pagamento, todavia, ressalvados os casos extremos, o curso legal costuma ser suficiente, desde que assegurado o poder liberatório da moeda para o pagamento de impostos".[10]

Na seção seguinte poderemos verificar como o mesmo truque ou âncora pode ser encontrado nas criptomoedas da segunda geração e em suas redes.

Tarifas nas redes blockchain da segunda geração

Todas as criptomoedas funcionam através de uma rede descentralizada que processa as transações de cada usuário. Convencionou-se chamar de criptomoedas da segunda geração aquelas cuja rede permite também o processamento de serviços. Assim, a primeira geração engloba as criptomoedas cuja rede somente processa as transações da sua própria criptomoeda, enquanto a segunda geração, além de processar transações, também oferece poder computacional para outros serviços.

Para que sejam processados os aplicativos é necessário que sejam pagas tarifas na própria criptomoeda da rede. Tais tarifas devem ser pagas ou pelos usuários ou pela carteira associada ao próprio aplicativo e o pagamento é proporcional ao gasto de poder computacional executado para uma determinada ação, remunerando os agentes

[9] Lerner, A. Money as a Creature of the State.
[10] Franco, G. A Moeda e a Lei.

responsáveis pelo processamento de dados. Além disso, elas visam a desincentivar os chamados *ataques econômicos*, nos quais um agente malicioso programa um aplicativo com um comando em *loop* que exige o gasto de um volume elevado de poder computacional.

Quanto maior o volume de serviços funcionando na rede, mais elevada será a demanda dos desenvolvedores e usuários pela criptomoeda nativa, pois tanto um quanto o outro precisarão armazená-la em uma certa quantidade nas suas carteiras para que seja abatida automaticamente a cada etapa do processamento de dados.

É possível estabelecer um paralelo entre a segunda citação de Abba Lerner neste capítulo e a estrutura de tarifas das criptomoedas da segunda geração. Este autor utilizou a palavra *truque* para descrever como o curso forçado e a cobrança de impostos levam à aceitação da moeda estatal. Os cidadãos aceitam uma moeda fiduciária porque sabem que todos os que tiverem obrigações com o Estado a demandarão para o pagamento de impostos e assim se cria um ciclo virtuoso de circulação monetária e de expectativas no qual ela se perpetua.

Fica fácil verificar que o mesmo fenômeno ocorre dentro de algumas redes blockchain. Se um desenvolvedor deseja instalar um serviço numa dessas redes, ele precisa da criptomoeda nativa. Outros indivíduos na qualidade de investidores e usuários desta moeda, sabem disso e criam a expectativa de que a moeda será continuamente demandada por desenvolvedores e usuários de serviços e, com isso, sentem-se mais confortáveis em poupar este criptoativo e a utilizá-lo em suas transações. A âncora está criada.

V. Conclusão

O quadro histórico atual é de grandes transformações e inovações no campo das moedas e das finanças e as criptomoedas são parte deste processo. Da mesma maneira que no passado, foi preciso estabelecer uma ponte entre a ciência econômica e o direito monetário para se chegar a uma fundamentação teórica para a moeda fiduciária, hoje é necessário encontrar canais de comunicação e uma linguagem para que economistas e profissionais de TI possam dialogar acerca de temas de interesse comum.

O autor espera ter contribuído para a compreensão dos fenômenos econômicos que se desenvolvem dentro do universo das criptomoedas da segunda geração, demonstrando que as teorias desenvolvidas no passado podem explicar o que ocorre em um área tão nova e tão promissora. Essa contribuição poderá ajudar tanto economistas que pensem em adicionar conhecimento teórico a este tópico de pesquisa, como também permitirá que profissionais de programação, criptografia e engenharia construam uma estrutura de pensamento para compreender melhor a matéria.

Podemos nos questionar se não foi a falta de fundamentação teórica em economia que levou ao fim precoce diversos projetos de criptomoedas que embora fossem promissores do ponto de vista da tecnologia, careciam de incentivos econômicos endógenos que viabilizassem a sua perpetuação no longo prazo. Alguns deles foram identificados neste trabalho, como o staking e as tarifas pagas por serviços instalados em redes blockchain.

Ainda não sabemos como será a criptoeconomia quando ela se consolidar como um setor. Ainda há muitas inovações em fase experimental, tais como empréstimos em criptomoedas, corretoras descentralizadas, tokens que representam ativos reais (imóveis e obras de arte, por exemplo), eleições em redes blockchain, stable coins (moedas ou metais tokenizados), etc. Quaisquer que sejam os desenvolvimentos que venham a nos surpreender, eles certamente poderão ser explicados pela teoria econômica através de paralelos com as moedas do passado ou do presente.

Da mesma maneira sempre encontraremos um fio condutor na história da moeda, identificando aspectos das moedas do futuro que sempre estiveram presentes nas

moedas primitivas. Isto foi o que se tentou demonstrar quando se apresentou a moeda como um registro, algo que já se manifestava nas moedas *físicas*, mas que só passou a transparecer à medida que os padrões monetários foram se tornando mais abstratos até chegarem às moedas digitais e criptomoedas que são tão somente registros eletrônicos.

VI. Referências bibliográficas

ANTONOPOULOS, Andreas; WOOD, Gavin. *Mastering Ethereum*, O'Reilly, 2ª edição, 2020.

FRANCO, Gustavo H. B. *A Moeda e a Lei*. Rio de Janeiro: Zahar, 2017.

FRANCO, Gustavo H. B. *O Desafio Brasileiro: ensaios sobre Desenvolvimento, Globalização e Moeda*. São Paulo: Editora 34, 1999.

HAYEK, Friedrich. *Denationalization of Money – Argument Refined*. London: The Institute of Economic Affairs, 3ª edição, 1990.

KNAPP, Georg F. *The State Theory of Money*, London: Macmillan & Company Limited, 1924.

LERNER, Abba. *Money as a Creature of the State*, Papers and Proceedings of the Fifty-ninth Annual Meeting of the American Economic Association, The American Economic Review, v. 37, pp. 312-217 maio, 1947.

MANN, Frederick. *The Legal Aspect of Money*, Oxford: Clarendon Press, 5ª edição, 1992.

MENGER, Karl. *On The Origin of Money*. The Economic Journal, pp.239-255, 1892.

MISHKIN, Frederic; MATTHEWS, Kent; GIULIODORI, Massimo. *The Economics of Money, Banking & Financial Markets*. Harlow: Pearson, European Edition, 2013

NAKAMOTO, Satoshi. *Bitcoin, a peer-to-peer electronic cash system*. Disponível em: <www.bitcoin.org, 2009 >

NIEBYL, Karl H. *Studies in the Classical Theories of Money*. New York: Columbia University Press, 1946.

Cardano documentation. Disponível em: <docs.cardano.org>

Ethereum White Paper. Disponível em: <https://ethereum.org/en/whitepaper>

Neo White Paper. Disponível em: <docs.neo.org>

ASIA TIMES. *Bitcoin price surge linked to China crackdown*. Disponível em: < https://asiatimes.com/2020/11/bitcoin-price-surge-linked-to-china-crackdown >